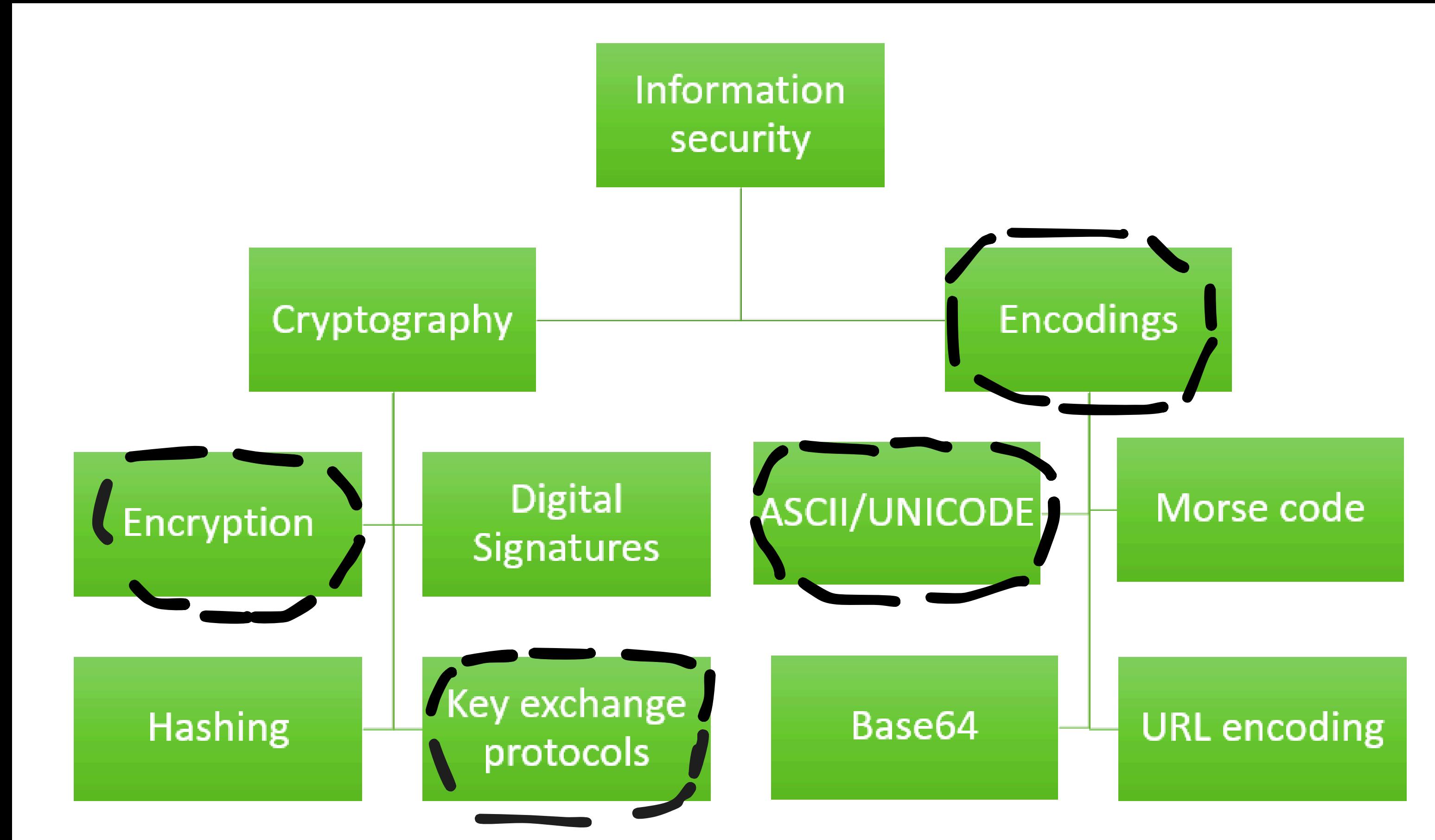
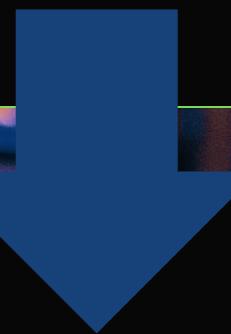


Updates - Submissions + Challenge cards
Week ahead and how people need to get familiar



CRYPTOGRAPHY

The science of securing communication through techniques like encryption, hashing, and digital signatures.



ENCRYPTION

A method within cryptography that transforms readable data (plaintext) into unreadable data (ciphertext) using a key, to ensure confidentiality.

ENCODINGS

The process of converting data into a different format for transmission, using publicly known rules — not meant for secrecy.

**OUR FOCUS
WITHIN
INFO
SECURITY**

ENCODINGS

Below are historical ciphers that once served encryption purposes, but no longer meet modern definitions due to lack of a secret key and low security.

ATBASH CIPHER

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	L	K	J	I	H	G	F	E	D	C	B	A

● ALPHABET ● ATBASH

Each letter in the alphabet is mapped to its reverse counterpart ($A \leftrightarrow Z$, $B \leftrightarrow Y$, $C \leftrightarrow X$, etc.).

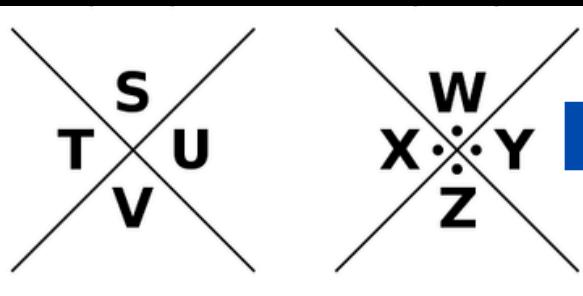
Decipher:

1. FNYIVOONZ
2. NZTRX

PIGPEN CIPHER

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R



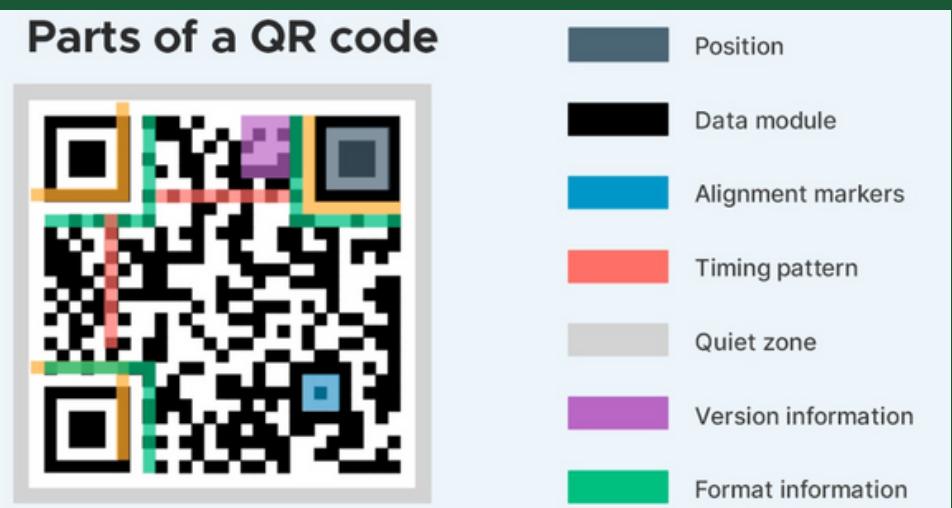
Pigpen Cipher is a geometrical monoalphabetic substitution cipher.

Decipher:

EF J Q O V
B D V V G

Any uniquely reversible mapping is a valid form of encoding data.

QR CODES



BASE64

BASE64 INDEX TABLE							
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Make your own!

Remember: You should always be able to retrieve the original data uniquely.

ASCII ENCODING

A → 65

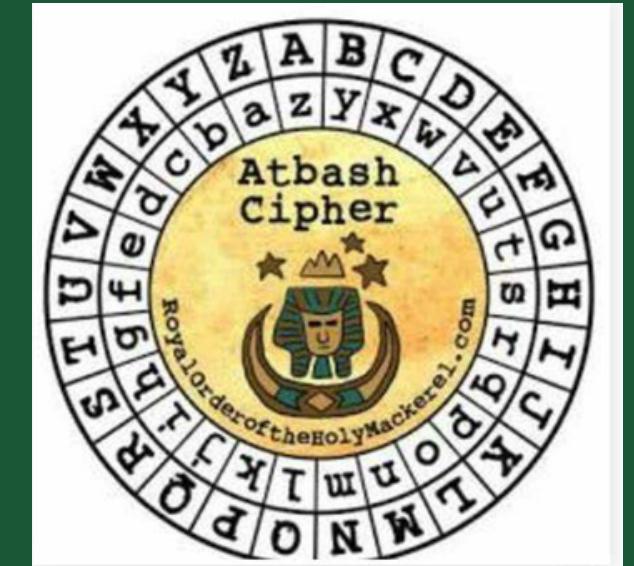
B → 66

C → 67

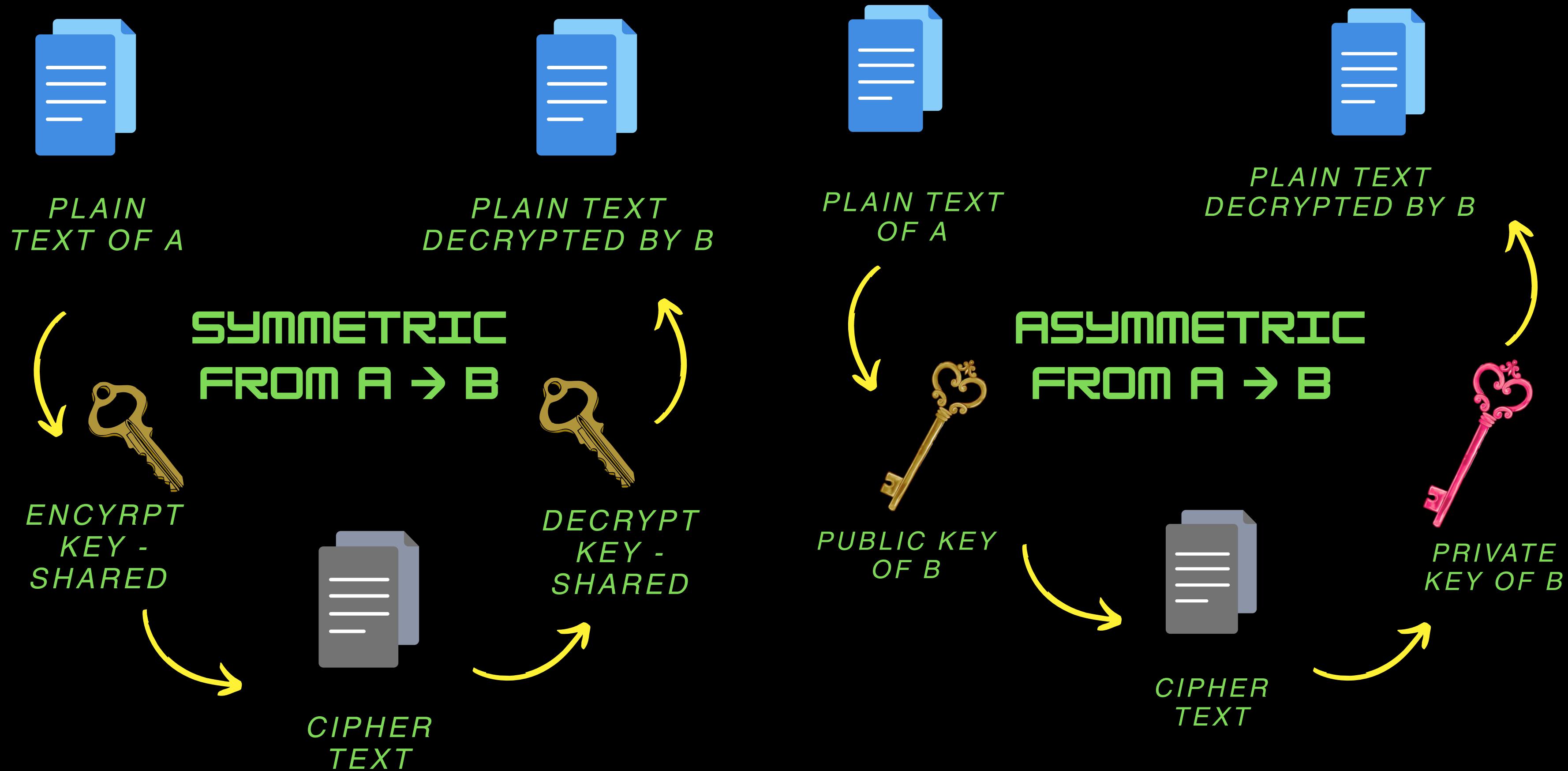
...

ATBASH, PIGPEN

A	• -	P	• - - - .	1	• - - - -
B	- - - .	Q	- - - - .	2	• - - - -
C	- - - . -	R	- - - - -	3	• - - - -
D	- - - - .	S	• - - - -	4	• - - - -
E	•	T	-	5	• - - - -
F	• - - - .	U	• - - - -	6	• - - - -
G	- - - - .	V	• - - - -	7	• - - - -
H	• - - - - .	W	• - - - -	8	• - - - -
I	• •	X	• - - - -	9	• - - - -
J	-	Y	• - - - -	0	• - - - -
K	- - - .	Z	- - - - .		
L	- - - - .				
M	- - - - - .				
N	- - - - - - .				
O	- - - - - - - .				
		?	• - - - -		
		/	- - - - -		
		=	- - - - -		

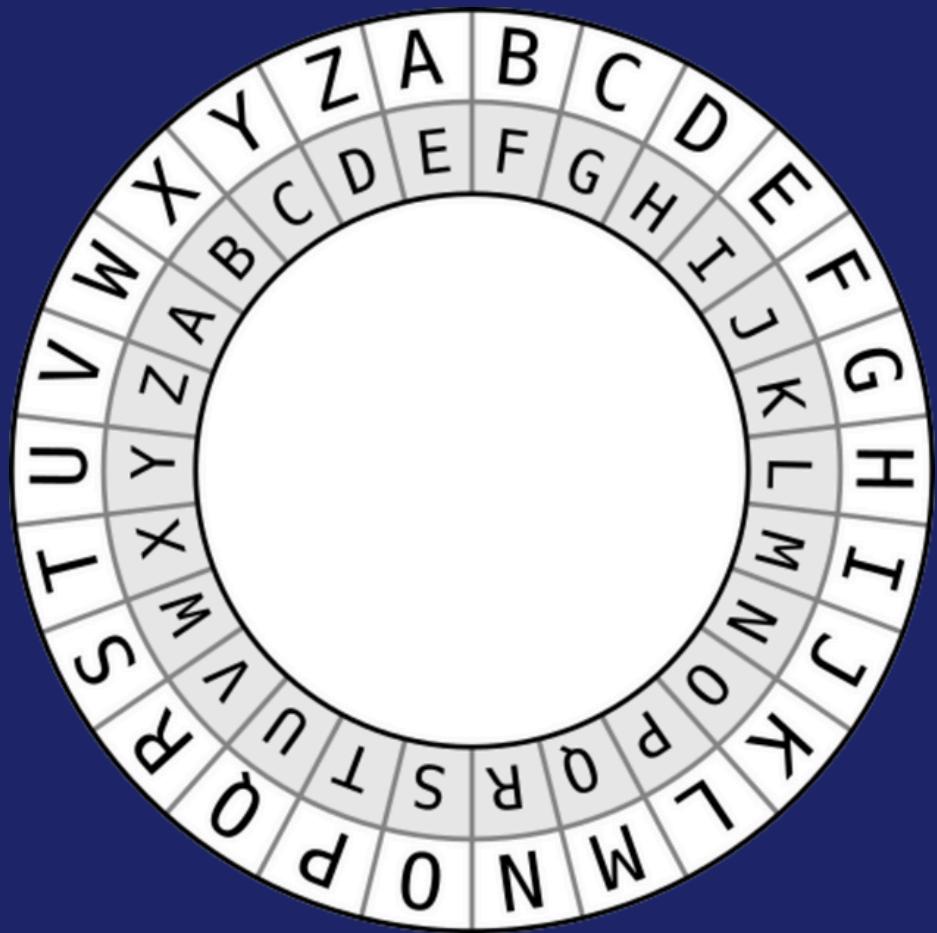


ENCRYPTION TECHNIQUES



SYMMETRIC ENCRYPTION TECHNIQUES

Caesar Cipher *SHIFT KEY = 4*



Wrap the alphabet around in a circle and push each letter ahead by shift key

Examples:

A → E

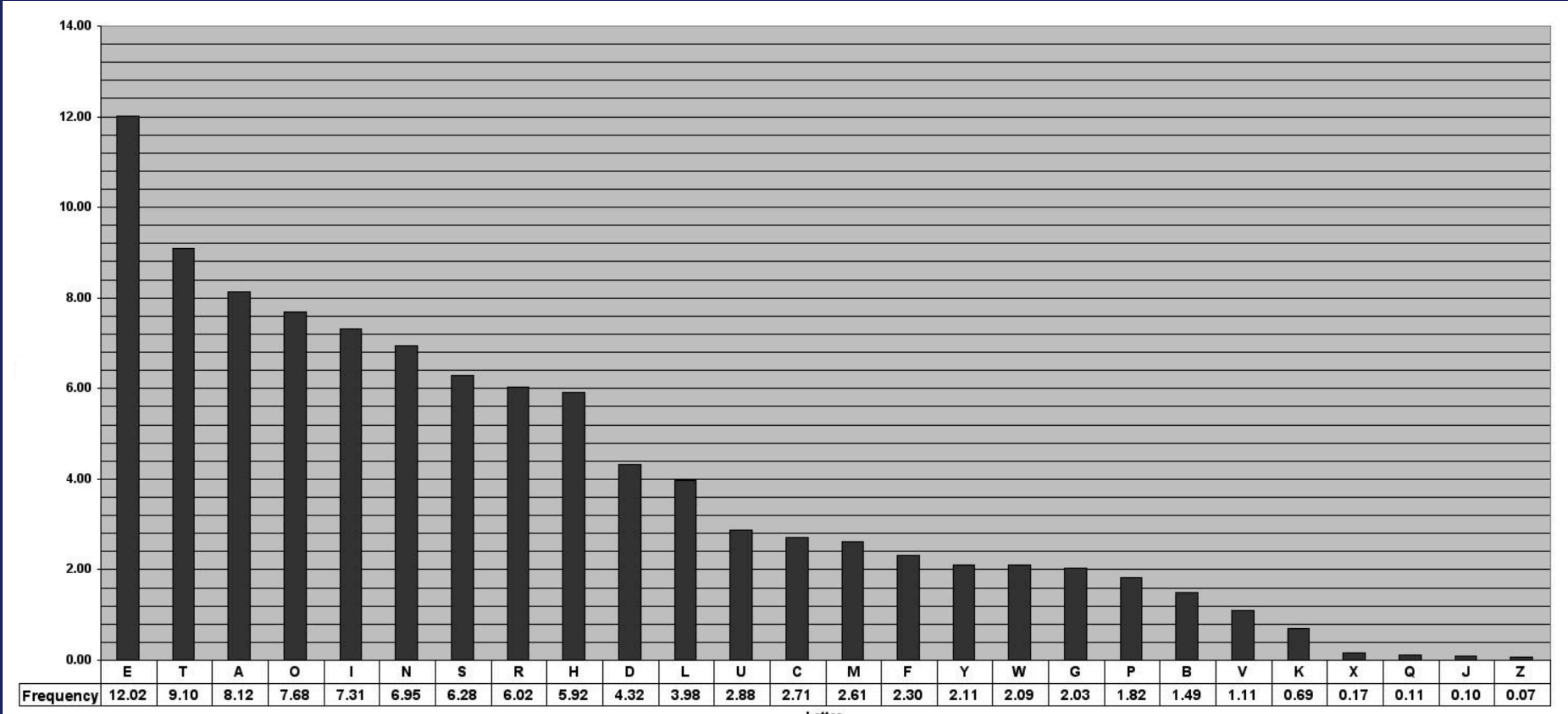
B → F

Z → D (due to the wrap around)

THINK!! 

What would happen if we have a negative shift key?
If you could make certain assumptions of the plain-text, can you decrypt the message without knowing the key?

Hint: How can we use the frequency of letters in the English Language?



VIGENÈRE CIPHER

- ▶ Key (K) : FRINGE
- ▶ Plain text(P): get all soldier a meal.
- ▶ Cipher text(C):

Note: This Vigenere is $P[i] + K[i]$



How does Vigenère's use of multiple shifts change letter frequency patterns compared to Caesar's single shift, and why does that make it harder to break?



What aspects of symmetric encryption make it susceptible to attack?

Think:

How do the sender and receiver agree upon a shared key without a listening third party also knowing? (paint activity – explain clearly)



Think further:

Even if two people agree upon a secret shared key, is it possible for the passing message to be tampered with/be heard?



Think Further Still:

How can we resolve this situation?

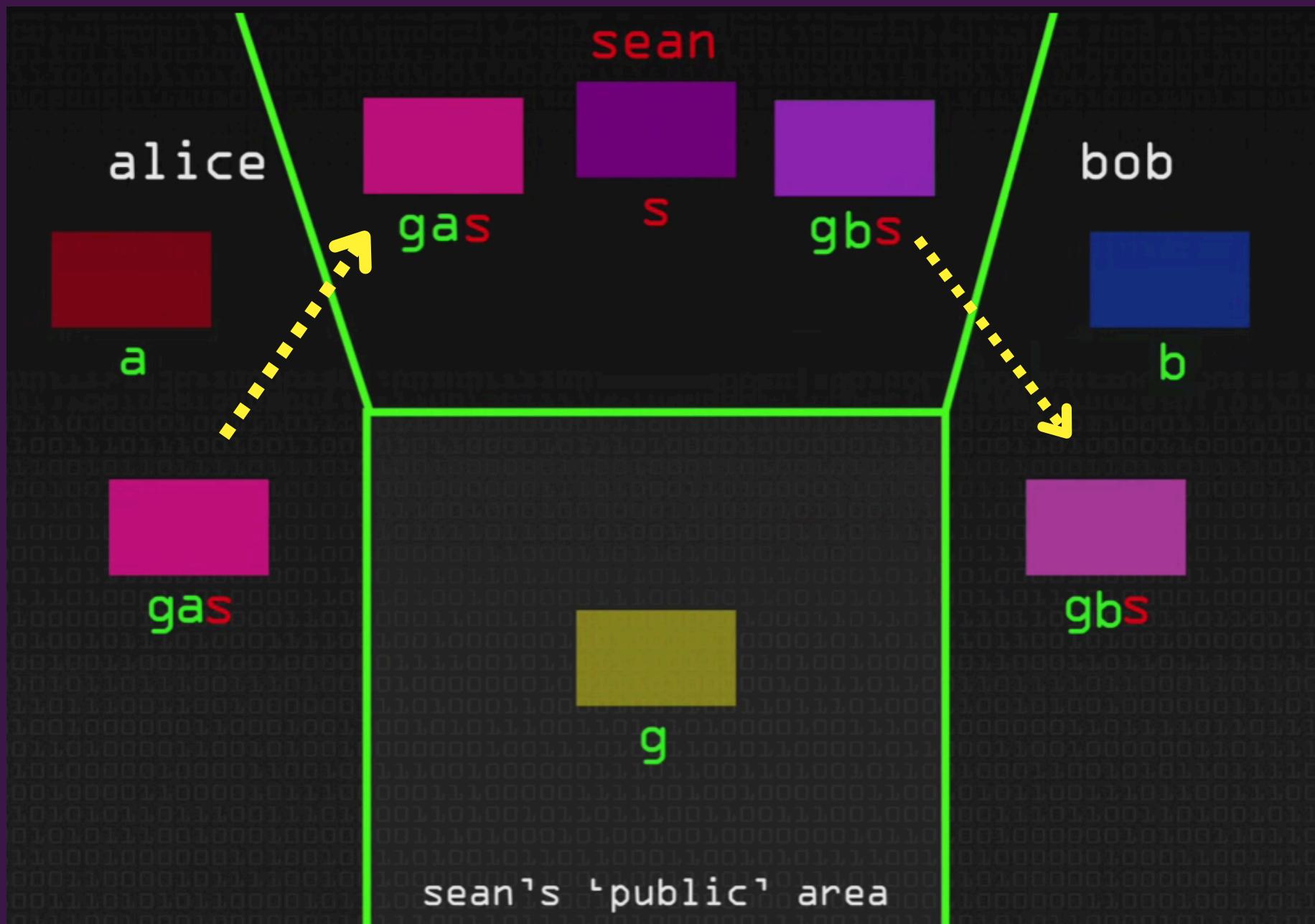
Diffie-Hellman to get shared secret key

starting from 2: 47 till end

Diffie-Hellman Key Exchange

Discrete Logarithm problem: it is difficult to know x after computing $g^x \text{ mod } n = m$ (this is the value sent across which can be intercepted)

Issue with Diffie Hellman Key Exchange



Sean acts as the middleman here and pretends to be Alice and Bob. He can overhear and even tamper with the conversations between them.

Need for identity proof
look into: digital signatures

ASYMMETRIC ENCRYPTION TECHNIQUES

<https://www.youtube.com/watch?v=hm8s6FAc4pg&t=224s>